

CLAIMS

1. A method for securing scrambled data supplied to a plurality of receiver terminals, each of said terminals comprising a plurality of descrambling modules M_j ($j = 1..M$), each having a specific processing capacity and a specific level of security, said data being previously subdivided into M families F_j ($j = 1..M$), each comprising N blocks B_i ($i = 1..N$) :
each block B_i ($i = 1..N$) of a family F_j being scrambled by a key K_j ($j = 1..M$) associated with the family F_j ,
said method characterised in that said blocks B_i ($i = 1..N$) are previously organised as a function of the respective processing speeds of the descrambling modules M_j .
- 15 2. The method as claimed in claim 1, characterised in that the modules M_j ($j = 1..M$) are different peripheral elements associated with said receiver terminal.
- 20 3. The method as claimed in claim 2, characterised in that the descrambling modules M_j ($j = 1..M$) comprise different algorithms A_j ($j = 1..M$).
- 25 4. The method as claimed in claim 2, characterised in that the descrambling modules M_j ($j = 1..M$) comprise identical algorithms A_j ($j = 1..M$).

5. The method as claimed in any one of Claims 1 to 4, characterised in that the data to be distributed are in the form of a previously stored file.

5 6. The method as claimed in any one of claims 1 to 4, characterised in that the data to be secured are in the form of a broadcast or downloaded stream and processed in real time by the terminal.

10 7. The method as claimed in claim 5 or 6, characterised in that the duration of use of the stream is divided into crypto periods, each corresponding to a descrambling key, and in that prior to each start of the crypto period a message is inserted into the stream 15 so as to warn the descrambling module M_j of the change in crypto period.

8. The method as claimed in claim 7, characterised in that said message comprises all information necessary for descrambling the stream utilised during 20 the following crypto period.

9. The method as claimed in any one of claims 1 to 8, characterised in that said data represent audio 25 and/or video programs protected by a DRM system.

10. The method as claimed in any one of claims 1 to 8, characterised in that said data represent images synthesis or animé drawings.

11. A system for securing scrambled data supplied to at least one receiver terminal, characterised in that it comprises:

a scrambling platform comprising:

5 - means for subdividing said data into m distinct families of N blocks B_i ($i = 1 \dots N$),

10 - means for assigning each family F_j a specific identification parameter p_j ($j = 1 \dots M$) associated with at least one descrambling module M_j having a specific processing capacity and a specific level of security,

15 - means for scrambling each block B_i by a key K_j ($j = 1 \dots M$) in biunivocal relation with the parameter p_j ,

and a descrambling platform comprising means for identifying the family of each block B_i so as to descramble each block B_i of a family of type p_j by the module M_j corresponding to said parameter p_j .

12. The system as claimed in claim 11,
20 characterised in that the descrambling distinct modules M_j ($j = 1 \dots M$) are distinct peripherals associated with the receiver terminal.

13. A scrambling platform for a stream of data,
25 characterised in that it comprises:

- means for subdividing said stream into m distinct families of N blocks B_i ($i = 1 \dots N$),

30 - means for assigning each family a specific identification parameter p_j ($j = 1 \dots M$) associated with at least one descrambling module M_j having a specific processing capacity and a specific level of security,

- means for scrambling each block B_i by a key K_j ($j = 1 \dots M$) in biunivocal relation with the parameter p_j .

5 14. The descrambling platform for a stream of data
scrambled by the platform of Claim 13, characterised in
that it comprises means for identifying the family of
each block B_i so as to descramble each block B_i of a
family of type p_j by the module M_j corresponding to
10 said parameter p_j .

15 15. The descrambling platform as claimed in claim
14, characterised in that it comprises a plurality of
distinct descrambling modules M_j ($i = 1 \dots M$) each
15 identified by the specific identification parameter p_j .

16. The descrambling platform as claimed in claim
15, characterised in that the receiver terminal is a
PDA and in that one of said descrambling modules M_j (i
20 $= 1 \dots M$) is integrated into the PDA and at least a
second module is a smart card of SIM type connected to
said PDA.

17. Utilisation of the process as claimed in any
25 one of claims 1 to 8 for securing a video-on-demand
service (VOD).

18. Utilisation of the process as claimed in any
one of claims 1 to 8 for securing a music-on-demand
30 service (MOD).

19. Utilisation of the process as claimed in any one of claims 1 to 8 for securing access to a broadcast service for electronic books either online or downloaded from portable media.